UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/830,127	04/22/2004	Paul A. Gassoway	063170.6962	7446

5073 7590 05/05/2010

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
05/05/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

Office Action Summary	Application No.	Applicant(s)	
	10/830,127	GASSOWAY, PAUL A.	
	Examiner	Art Unit	
	ELENI A. SHIFERAW	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *56-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/2/10*.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed 10/28/2009. Claims 1-5, 7-10, 12-21, 23-26, 28-37, 39-42 and 44-55 have been previously allowed on 03/23/2009 page 2 of the Non-Final Office action. Only the 101 rejection to claim 33 and intervening claims and 103 rejections to claims 50-60 are argued by the applicant remark submitted on 1/28/10.

Response to Arguments

2. Applicant's arguments filed 1/28/10 have been fully considered but they are not persuasive.

3. The applicant amends claim 33 and intervening claims as suggested by the examiner in the previous office action dated on 10/28/09 pages 3-4 and the 101 rejection is in compliance with the examiner's suggestion.

Regarding argument Berger failure to teach adding an entry to a database of known good software if the quantitative information exceeds a predetermined value, remark pages 14-15, argument is not persuasive because Berger does in fact make the determination that an application is safe based on quantitative information value. See par. 32-33 and 75 that discloses monitoring and analyzing actions of the various applications executing on the system to detect malicious actions based on RULES. The rules including:

> when **run once** key is accessed by the application;
> when the application opens itself;
> when **number of many same types** of files are opened or altered by the application; (i.e., exceeding predetermined amount of files to be open)
> when a **number of many bitmap or JPEG files are overwritten (exceeding predetermined number of overwriting)**;

when executable files are opened and modified ....
Berger further updates local configuration operation if application is safe or unsafe operation. In update local configuration operation 322, the local configuration, e.g., application characteristics, on server system 130 is updated to reflect that the potentially unsafe application is now a known safe application or a known unsafe application (see par. 68, 81 and fig. 2).

Regarding applicant's argument no motivation to combine Berger and Dutta, remark page 15, argument is not persuasive because Berger and Dutta are analogous in network monitoring and network data updating by making information current. Berger generates update to make the network information current, i.e., "updates .... to reflect that the potentially unsafe application is now a known unsafe application. (see par. 57)" Dutta updates to make the network information current, i.e., "updating ... throughout the peer to peer network (see col. 13 lines 55-59 & 63-67)."

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 56-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berger (US 2004/0123117) in view of Dutta et al (US 7,539,664).

Claim 56: Berger discloses a method for computer security, comprising:

identifying a file(paragraph [0084]);

i. determining whether an entry for the file exists in database of unfamiliar software(*If the application characteristic doesn't match either a known safe application characteristic or a known unsafe application characteristic, a determination is made in operation 208 that the potentially unsafe application is an unknown application)(paragraph [0047]; Fig. 3, steps 314-320)*;

ii. adding an entry for the file to a database of known good software if the quantitative information exceeds a predetermined value*(if application is safe or unsafe operation 320, flow moves to an update local configuration operation 322. In update local configuration operation 322, the local configuration, e.g., application characteristics, on server system 130 is updated to reflect that the potentially unsafe application is now a known safe application or a known unsafe application) (paragraphs [0068], [0081]);* and

iii. allowing the opening of the file to continue if the database of known good software includes the entry for the file(*paragraph[0084*]).

Berge does not explicitly discloses determining quantitative information regarding the file, the quantitative information selected from the group consisting of a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed. However Dutta et al discloses a method for operating a rating server, which determining quantitative information regarding the file, the quantitative information selected from the group consisting of a length of time the entry has been in the database of unfamiliar

software, a number of times the file has been opened, and a number of times an executable in the file has been *executed (the search result post-processor can monitor and record or log the number of times that a general file is opened or the number of times that an executable file has been executed. The search result post-processor could also monitor how long a file is kept before it is deleted (or moved) (column 9, lines 34-43).* Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Berger such as to use quantitative information. The motivation of doing so would have been to improve the performance of malicious computer code detection as taught by Dutta et al (column 1, lines 5-10).

Claim 57: Berger and Dutta et al disclose the method as in claim 56 above, and Burger further discloses a step of removing the entry for the file from the database of unfamiliar software if the quantitative information exceeds a predetermined value(paragraph [0084]: Fig 2).

Claim 58: Berger and Dutta et al disclose the method as in claim 56 above, and Burger further discloses a step of preventing the opening of the file to continue if:
the database of known good software does not include the entry for the file(terminating)(paragraph [0049]); and
the file attempts a suspicious activity(deleting a file)(paragraph [0045]).

Claim 59: Berger and Dutta et al disclose the method as in claim 58 above, and Burger further discloses wherein a suspicious activity comprises updating a registry(paragraph [0033]).

Claim 60: Berger and Dutta et al disclose the method as in claim 58 above, and Burger

further discloses wherein a suspicious activity comprises opening a second file(paragraph [0033]).

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 6:00am-2:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/
Primary Examiner, Art Unit 2436